

REPLY UNDER 37 CFR §1.116
EXPEDITED PROCEDURE
TECHNOLOGY CENTER 2600

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Ronald D Ryan et al.	§	Docket No.:	22171.375
		§		(12286RRUS01U)
Serial No.:	09/697,822	§	Examiner:	Shah, Chirag G.
Filed:	October 26, 2000	§	Art Unit:	2664
For:	System and Method for Reporting Communication Related Information in a Packet Information in a Packet Mode Communication	§ § § § §	Conf. No.:	6680

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Service

I hereby certify that this correspondence is being filed with
the U.S. Patent and Trademark Office via EFS-Web on
August 15, 2006.



Linda Ingram

AMENDMENT AFTER FINAL

Sir:

In response to the Final Office Action of June 9, 2006, please amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on **page 2** of this paper.

Remarks/Arguments begin on **page 10** of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for lawful interception of communication ~~related~~ information comprising:

selecting a location for intercepting a communication in a packet data network based at least in part on an event type;

detecting the occurrence of a predetermined event in said packet data network;

gathering ~~a set of communication related~~ information [[of]] ~~relating to a type of the predetermined event from~~ said communication at said selected location ~~based at least in part on a type of the detected event~~ in response to [[said]] detection of the occurrence of said ~~type of the predetermined event~~; and

transmitting said gathered communication ~~related~~ information to at least one law enforcement agency.

2. (Original) The method of claim 1, wherein said packet data network comprises a UMTS network.

3. (Original) The method of claim 1, wherein said interception is performed by a Surveillance Access Point (SAP).

4. (Original) The method of claim 1, wherein said selecting a location comprises intercepting said communication at a CSCF in said packet data network if the event is a call signaling event.

5. (Original) The method of claim 1, wherein said selecting a location comprises intercepting said communication at a serving node in said packet data network if the event is a path establishment or a path release.

6. (Original) The method of claim 5, wherein said serving node is selected from the group consisting of a SGSN and an E-SGSN.

7. (Original) The method of claim 1, wherein said selecting a location comprises intercepting said communication at a gateway node in said packet data network if the event is transmission of a packet.

8. (Original) The method of claim 7, wherein said gateway node is selected from the group consisting of a GGSN and an E-GGSN.

9. (Original) The method of claim 1, wherein said transmitting said gathered communication related information further comprises:

providing said gathered information to a delivery function;

formatting said gathered information by said delivery function into a format acceptable to said at least one law enforcement agency; and

forwarding said formatted information to said law enforcement agency.

10. (Original) The method of claim 9, wherein said delivery function utilizes a J-STD-025 interface.

11. (Original) The method of claim 3, wherein said transmitting said gathered communication related information comprises:

formatting said gathered information by said SAP into a report acceptable to said at least one law enforcement agency; and

providing said report to said law enforcement agency.

12. (Currently Amended) The method of claim 1, wherein the type of said detected predetermined event comprises call signaling, path establishment or path release, and transmission of a packet.

13. (Currently Amended) The method of claim 1, wherein said gathered communication ~~related~~ information includes information related to call signaling.

14. (Currently Amended) The method of claim 1, wherein said gathered communication ~~related~~ information includes information related to path establishment or path release.

15. (Currently Amended) The method of claim 1, wherein said gathered communication ~~related~~ information includes packet information.

16. (Original) The method of claim 13, wherein said call signaling information includes information indicating the type of signaling, wherein said information is selected from the group consisting of H.323 and SIP.

17. (Original) The method of claim 14, wherein said path establishment information includes information indicating the status of a path between a mobile terminal and said packet network, wherein said information is selected from the group consisting of established and released.

18. (Original) The method of claim 15, wherein said packet information includes a source address and a destination address of a packet.

19. (Currently Amended) A method for lawful interception of communication related information, comprising:

detecting the occurrence of an event in a packet data network;

collecting a set of communication related information [[of]] relating to a type of the event from a communication in said packet data network in response to said detection of [[an]] the type of the event based at least in part on a type of said detected event; and

providing said collected communication relating information to one or more law enforcement agencies.

20. (Original) The method of claim 19, wherein said packet data network includes a UMTS network.

21. (Original) The method of claim 19, wherein said detected event is a call signalling event and said collected communication related information includes information selected from the group consisting of H.323 and SIP, and information selected from the group consisting of a time stamp for the detection of the occurrence of said event, a session identifier, and an identifier of the type of the communication.

22. (Original) The method of claim 19, wherein said detected event is selected from the group consisting of the establishment of a path and release of a path, wherein said collected communication relating information includes a path related information, wherein said path related information is selected from the group consisting of path established and path released, wherein said collected information further includes information selected from the group consisting of a time stamp for the detection of the occurrence of said event, and a path identifier for said path.

23. (Original) The method of claim 19, wherein said detected event is transmission of a packet in said packet data network, wherein said packet includes a payload and a network layer, and wherein said collected communication related information includes information selected from the group consisting of source address of said packet and a destination address of said packet.

24. (Original) The method of claim 23, wherein said information further includes information selected from the group consisting of a path identifier for a path utilized for said transmission of said packet and an address of a network service to which said packet is delivered prior to being delivered to said destination address.

25. (Original) The method of claim 19, wherein said providing comprises:
providing said collected information to a delivery function;
formatting said collected information by said delivery function into a format acceptable to said one or more law enforcement agencies; and
providing said formatted information to said one or more law enforcement agencies.

26. (Currently Amended) A system for lawful interception of communication related information, comprising:
means for detecting the occurrence of an event in a packet data network;
means for collecting a set of communication related information [[of]] relating to a type of the event from a communication in said packet data network in response to said detection of the type of the [[an]] event based on a type of said detected event; and
means for providing said collected information to one or more law enforcement agencies.

27. (Currently Amended) A system for lawful interception of communication related information, comprising:

a base station for receiving an event from an intercept device in a packet mode data network;

a node operable to communicate with said base station; and

a surveillance access point (SAP) operable to communicate with said node, wherein said SAP intercepts a communication upon the detection of said event in said packet mode data network, and wherein said SAP gathers ~~a set of communication related~~ information [[of]] ~~relating to a type of the event from~~ said intercepted communication ~~based on a type of the event upon the detection of the type of the event~~ and provides said gathered information to a law enforcement agency.

28. (Original) The system of claim 27, wherein said base station is a Radio Access Network.

29. (Original) The system of claim 27, wherein said intercept device is a mobile terminal selected from the group consisting of a wireless phone, a personal digital assistant, and a pager.

30. (Original) The system of claim 27, wherein said node is a serving node.

31. (Original) The system of claim 27, wherein said node is a SGSN.

32. (Original) The system of claim 27, wherein said SAP is part of a node selected from the group consisting of a serving node and a gateway node.

33. (Original) The system of claim 27, wherein said SAP is part of a node selected from the group consisting of a serving GPRS support node, an extended serving GPRS support node, a gateway GPRS support node, and an extended gateway GPRS support node.

34. (Currently Amended) The system of claim 27, wherein said gathered communication ~~related~~ information includes information about the initiation of a call setup by said intercept device.

35. (Currently Amended) The system of claim 27, wherein said gathered communication ~~related~~ information includes information about the initiation of a session setup by said intercept device.

36. (Currently Amended) The system of claim 27, wherein said gathered communication ~~related~~ information includes information about the establishment of a communication path between said intercept device and a network service.

37. (Currently Amended) The system of claim 27, wherein said gathered communication ~~related~~ information includes information about the release of a communication path between said intercept device and a network service.

38. (Currently Amended) The system of claim 27, wherein said gathered communication ~~related~~ information includes the destination address of a packet transmitted over a communication path between said intercept device and a network service.

39. (Original) The system of claim 38, wherein said destination address is the address of said network service.

40. (Original) The system of claim 38, wherein said destination address is the address of another device associated with said network service and said gathered information further includes an address of said network service, wherein said packet is delivered to said another device via said network service.

41. (Original) The system of claim 38, wherein said network service is associated with an Internet Service Provider (ISP).

42. (Original) The system of claim 38, wherein said destination address is the address of an associate device.

REMARKS

Claims 1-42 remain in this application. Claims 1, 19, and 26-27 are amended to recite “gathering a set of communication information relating to a type of the predetermined event from said communication at said selected location in response to said detection of the occurrence of said type of the predetermined event.” These features are supported at least on page 14, lines 14-15 of the current specification. No new matter is added as a result of the above amendments. Reconsideration of this application in light of the above amendments and the following remarks is requested.

Rejections Under 35 U.S.C. §103(a), Claims 1-3, 5-8, 12, 14-15, 17, 18-20, 22-24, and 26

Claims 1-3, 5-8, 12, 14-15, 17, 18-20, 22-24, and 26 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Sjoblom (U.S. Publication No. 2002/0150096) in view of newly cited reference by Hippelainen (U.S. Publication No. 2002/0078384). This rejection is respectfully traversed.

As the PTO recognizes in MPEP § 2142:

... The examiner bears the initial burden of factually supporting any prima facie conclusion of obviousness. If the examiner does not produce a prima facie case, the applicant is under no obligation to submit evidence of nonobviousness...

It is submitted that, in the present case, the examiner has not factually supported a prima facie case of obviousness for the following, mutually exclusive, reasons.

1. Even When Combined, the References Do Not Teach the Claimed Subject Matter

The Sjoblom and Hippelainen references cannot be applied to reject claims 1, 19, and 26 under 35 U.S.C. § 103 which provides that:

A patent may not be obtained ... if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains ... (Emphasis added)

Thus, when evaluating a claim for determining obviousness, all limitations of the claim must be evaluated. Neither Sjoblom nor Hippelainen discloses or suggests “gathering a set of communication information relating to a type of the predetermined event from said communication at said selected location in response to said detection of the occurrence of said type of the predetermined event,” as is claimed in claims 1, 19, and 26 it is impossible to render the subject matter of claims 1-3, 5-8, 12, 14-15, 17, 18-20, 22-24, and 26 as a whole obvious, and the explicit terms of the statute cannot be met.

The examiner admits that Sjoblom does not disclose such features, but alleges that Hippelainen discloses these features in paragraphs 60-61, which read as follows:

According to FIG. 3, an initial interception request is issued from the LEA to the LIG. In fact, the LEA passes a lawful authorization to the network operator, access provider or service provider. The network operator, access provider or service provider determines the relevant target identities from the information given in the lawful authorization. Then, the network operator, access provider or service provider commands an interception control unit, used for controlling the interception functions of the LINs, to provide a corresponding interception information to the LIN of the relevant target identity. The interception control unit can be arranged in the LEA (as in the case of FIG. 3) or in a separate network element.

Subsequently, the interception control unit transmits the required LIN settings via the packet network to the corresponding LIN. In response to the receipt of the LIN settings, the LIN performs a packet interception and duplicates those packets which are to be intercepted based on their header information. Then, the intercepted packets are encrypted and fake packets are generated and added to the intercepted packets. These encrypted and blurred data packets are transmitted via corresponding interworking units (IWU) through the ATM WAN to the LIG. Due to the encryption processing, a secure tunnel is established, although the intercepted data packets are transmitted via a normal channel of the packet network. (Emphasis added)

Paragraphs 60-61, Hippelainen.

Fig. 3 of Hippelainen is shown below:

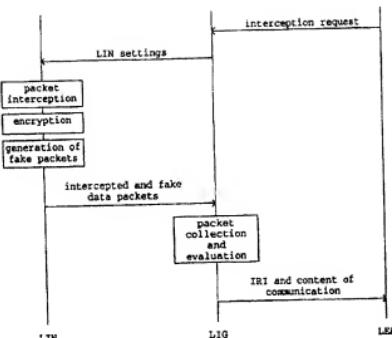


Fig. 3

In the above section and in Fig. 3, Hippelainen discloses that the lawful interception node (LIN) intercepts the packet and duplicates the intercepted packet based on the header information. The LIN then encrypts the intercepted packet and adds generated fake packets to the intercepted packet. Contrary to the examiner's allegation, the LIN gathers all the information from the packets each time they are intercepted by duplicating them. Hippelainen does not gather a set of communication information from the packet relating to the type of event detected.

Instead, Hippelainen duplicates all the information from the packet and encrypts the entire intercepted packet. This is different from the presently claimed features in that Hippelainen gathers all the information available from the packet instead of gathering a set of information that is related to the type of detected event. For example, if the detected event type is call signalling, the information in Table I relating to call signalling is gathered. If the detected event type is establishment or release of packet mode communication path, the information in Table II relating to the establishment or release of packet mode communication is gathered. Hippelainen does not disclose such features as recited in amended claims 1, 19, and 26.

Furthermore, the examiner alleges that it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Sjoblom to include gathering a set of communication information relating to the type of detected event such as a

transmission of a packet as taught by Hippelainen, because one is motivated as such in order to intercept the relevant target identify packets to make available results of interception relating to a specific identifies to a Law Enforcement Agency. Applicants respectfully disagree.

As discussed above, Hippelainen is only interested in duplication all the information from the packets that are identified in the header information. Hippelainen does not gather a set of information from the intercepted packet relating to the type of detected event. This is because Hippelainen is only interested in “a packet reading means 11 where the header of the extracted data packets is read and analyzed as to whether the data packet should be intercepted or not.” (Paragraph 66). Hippelainen is not interested in gathering a set of communication information that relates to the type of detected event. Therefore, one of ordinary skill in the art would not have been led to combine the disclosures of Sjoblom and Hippelainen to reach the features of claims 1, 19, and 26.

Accordingly, for at least this reason, Sjoblom and Hippelainen are insufficient to provide a *prima facie* case of obviousness with regard to claims 1-3, 5-8, 12, 14-15, 17, 18-20, 22-24, and 26. For the reasons described above, the examiner’s burden of factually supporting a *prima facie* case of obviousness has clearly not been met, and the rejection under 35 U.S.C. §103 should be withdrawn.

2. The Combination of References is Improper

There is still another reason why the Sjoblom and Hippelainen references cannot be applied to reject claims 1-3, 5-8, 12, 14-15, 17, 18-20, 22-24, and 26 under 35 U.S.C. § 103(a).

§ 2142 of the MPEP also provides:

...the examiner must step backward in time and into the shoes worn by the hypothetical ‘person of ordinary skill in the art’ when the invention was unknown and just before it was made....The examiner must put aside knowledge of the applicant’s disclosure, refrain from using hindsight, and consider the subject matter claimed ‘as a whole’.

Here, neither Sjoblom nor Hippelainen discloses, or even suggests, the desirability of the combination since neither discloses “gathering a set of communication information relating to a type of the predetermined event from said communication at said selected location in response to said detection of the occurrence of said type of the predetermined event” as is claimed in

claims 1, 19, and 26. As discussed above, Hippelainen merely duplicates all the information in the packets that are identified in the header information. Hippelainen does not gather a set of communication information from the packet relating to the type of detected event.

Thus, it is clear that neither patent provides any incentive or motivation supporting the desirability of the combination. Therefore, there is simply no basis in the art for combining the references to support a 35 U.S.C. § 103 rejection.

In this context, the MPEP further provides at § 2143.01:

The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination.

In the above context, the courts have repeatedly held that obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching, suggestion or incentive supporting the combination.

In the present case it is clear that the examiner's combination arises solely from hindsight based on the invention without any showing, suggestion, incentive or motivation in either reference for the combination as applied to claims 1-3, 5-8, 12, 14-15, 17, 18-20, 22-24, and 26. Therefore, for this mutually exclusive reason, the examiner's burden of factually supporting a *prima facie* case of obviousness has clearly not been met, and the rejection under 35 U.S.C. §103 should be withdrawn.

For the reasons described above, Sjoblom and Hippelainen do not render the claims *prima facie obvious*, and the rejections of claims 1-3, 5-8, 12, 14-15, 17, 18-20, 22-24, and 26 under 35 U.S.C. §103 should be withdrawn.

Rejections Under 35 U.S.C. §103(a), Claims 9, 11, 13, 25, and 27-42

Claims 9, 11, 13, 25, and 27-42 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Sjoblom in view of Hippelainen and further in view of Prieur (U.S. Patent No. 6,470,075). This rejection is respectfully traversed.

As the PTO recognizes in MPEP § 2142:

... The examiner bears the initial burden of factually supporting any prima facie conclusion of obviousness. If the examiner does not produce a prima facie case, the applicant is under no obligation to submit evidence of nonobviousness...

It is submitted that, in the present case, the examiner has not factually supported a prima facie case of obviousness for the following, mutually exclusive, reasons.

1. Even When Combined, the References Do Not Teach the Claimed Subject Matter

The Sjoblom and Hippelainen references cannot be applied to reject claims 9, 11, 13, 25, and 27-42 under 35 U.S.C. § 103. As discussed above in arguments presented for claims 1, 19, and 26, neither Sjoblom nor Hippelainen discloses or suggests “gathering a set of communication information relating to a type of the predetermined event from said communication at said selected location in response to said detection of the occurrence of said type of the predetermined event,” as is claimed in claims 1, 19, and 26. Prieur also does not disclose such features

The examiner alleges that Prieur discloses these features at column 3, line 60 to column 4, line 7, column 4, lines 54-56, and column 5, line 49 to column 6, line 2, which read as follows:

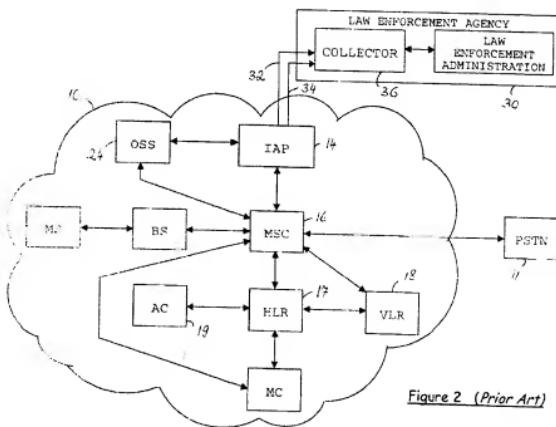
The access sub-function 12, shown in Fig. 1, is typically embodied as one or more Intercept Access Point (IAPs) 14, connected to the appropriate nodes of the cellular telecommunication network 10, as shown in Fig. 2, or to the PSTN nodes (not shown). Typically, these nodes may be mobile switching centers (MSCs) 16, as shown in Fig. 2, since MSCs 16 are the core of the cellular telecommunication network, and voice and data communication always go through at least one MSC where they are most likely to be intercepted. The IAP is typically provided as a node within the cellular telecommunication network 10, or the PSTN 11, where the communications of a monitored subscriber are accessed. Alternatively, the IAP may be co-located with the MSC 16. Column 3, line 60 to column 4, line 7, Prieur.

Therefore, it is logical that IAP 14 is connected to the MSC 16, in order to be able to intercept communications of monitored subscribers.
Column 4, lines 54-56, Prieur.

Continuing to refer to Fig. 2, once the call content and the call identification information are intercepted by the IAP 14, they are typically delivered, through the delivery function 18 to the Law Enforcement Agency 30. As stated, the delivery function 18 may also be provided as a software tool implemented as part of the MSC 16 or the IAP 14. Alternatively, the delivery function may comprise dedicated hardware circuitry for delivering the intercepted information to the LEA 30. As described in the foregoing, the delivery function 18 is associated with the delivery network comprising call content channel 32 for delivering the call content information, such as the voice and data information, and the call data channel 34 for delivering the call identifying information.

The delivery function 18 delivers the intercepted information of the monitored subscriber to LEA 30 (only one LEA is shown on Fig. 2, although various LEAs may be connected to the same cellular telecommunication network 10). A collector module 36 performs the collection function 20 within the LEA, before forwarding the intercepted information to the LEA administration 26.
Column 5, line 49 to column 6, line 2, Prieur.

Fig. 2 of Prieur is shown below:



In the above sections and in Fig. 2, Prieur merely discloses an IAP that delivers intercepted information to the Law Enforcement Agency via the delivery function and a collector module within the LEA that performs collection function 20, which collects and analyzes the

intercepted communication and the call-identifying information of the monitored subscribers for a particular LEA (column 4, lines 20-24).

However, nowhere in the reference does Prieur mention that “a SAP that gathers a set of communication information relating to a type of the event from said intercepted communication upon the detection of the type of the event,” as recited in claim 27. To the contrary, Prieur specifically discloses, at column 4, lines 39-43, that “the collection sub-function 20 is under the responsibility of the LEAs.” Therefore, it is the LEAs that collect the information sent by the cellular operators from the delivery sub-function 18.” Thus, instead of a SAP that gathers the communication information, Prieur discloses that the information is collected by the LEAs. Since Prieur does not disclose a SAP that gathers communication information, Prieur does not and would not disclose a SAP that gathers a different type of communication information relating to a type of the event. Therefore, Prieur also does not disclose or suggest the features of claim 27.

In addition, the examiner alleges that it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Sjoblom to include the features of performing the functionalities as taught by Prieur in order for the LEAs to find potentially incriminating information relating to the monitored subscribers in real time without prolonged delay. Applicants respectfully disagree.

Sjoblom merely discloses gathering all necessary interception related information (intercepted data) from the communication and generating a data packet. There is no mention of a type of the event, let alone gathering a set of communication information relating to a type of the detected event. Prieur, on the other hand, merely discloses a collector module within a LEA that collects intercepted information, not a SAP that gathers communication information. Therefore, Prieur does not and would not disclose a SAP that gathers a set of communication information relating to a type of detected event. One of ordinary skill in the art would not have been led to modify the teachings of Sjoblom to include Prieur’s collector module, because Prieur’s collector module for collecting communication information is within a LEA, not a SAP. In addition, neither reference mentions gathering a set of communication information relating to an event type. Therefore, one of ordinary skill in the art would not have been led to include the feature of claim 27, as alleged by the examiner.

Accordingly, for at least this reason, Sjoblom, Hippelainen, and Prieur, either alone or in combination, are insufficient to provide a *prima facie* case of obviousness with regard to claims 9, 11, 13, 25, and 27-42. For the reasons described above, the examiner's burden of factually supporting a *prima facie* case of obviousness has clearly not been met, and the rejection under 35 U.S.C. §103 should be withdrawn.

2. The Combination of References is Improper

There is still another reason why the Sjoblom, Hippelainen, and Prieur references cannot be applied to reject claims 9, 11, 13, 25, and 27-42 under 35 U.S.C. § 103(a).

Here, Sjoblom, Hippelainen, and Prieur also fail to disclose, or suggest, the desirability of the combination since neither discloses "a surveillance access point (SAP) operable to communicate with said node, wherein said SAP gathers a set of communication information relating to a type of the event from said intercepted communication upon the detection of the type of the event" as is claimed in claims 1, 19, 26, and 27 from which claims 9, 11, 13, 25, and 28-42 depend. As discussed above, Hippelainen merely duplicates all the information in the packets that are identified in the header information. Hippelainen does not gather a set of communication information relating to a type of detected event. Prieur merely discloses a LEA, not a SAP, that gathers all intercepted information.

Thus, it is clear that none of the references provides any incentive or motivation supporting the desirability of the combination. Therefore, there is simply no basis in the art for combining the references to support a 35 U.S.C. § 103 rejection. In the above context, the courts have repeatedly held that obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching, suggestion or incentive supporting the combination.

In the present case it is clear that the examiner's combination arises solely from hindsight based on the invention without any showing, suggestion, incentive or motivation in either reference for the combination as applied to claims 9, 11, 13, 25, and 27-42. Therefore, for this mutually exclusive reason, the examiner's burden of factually supporting a *prima facie* case of obviousness has clearly not been met, and the rejection under 35 U.S.C. §103 should be withdrawn.

For the reasons described above, Sjoblom, Hippelainen, and Prieur, either alone or in combination, do not render the claims *prima facie obvious*, and the rejections of claims 9, 11, 13, 25, and 27-42 under 35 U.S.C. §103 should be withdrawn.

Conclusion

It is clear from all of the foregoing that independent claims 1, 19, 26, and 27 are in condition for allowance. Dependent claims 2-18, 20-25, and 28-42 depend from and further limit independent claims 1, 19, and 27 and therefore are allowable as well.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,



Wing Y Mok
Registration No. 56,237

Dated: August 15, 2006

HAYNES AND BOONE, LLP
901 Main Street, Suite 3100
Dallas, Texas 75202-3789
Telephone: 972/739-8626
Facsimile: 972/692-9075

Attorney Docket No. 22171.375